



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:

5500

ARS

19 SEP 2013

Security Note 04-13

From: Director, Administration and Resource Management Division

Subj: HEADQUARTERS, U.S. MARINE CORPS (HQMC) INFORMATION,
PERSONNEL, AND PHYSICAL SECURITY ASSESSMENT PROGRAM

Ref: (a) SECNAV M-5510.36
(b) SECNAV M-5510.30
(c) DOD M-5200.01
(d) HQMC IPSP SOP

Encl: (1) Detailed Inspection Checklist

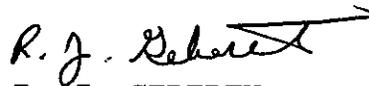
1. The HQMC Information, Personnel, and Physical Security Assessment Program is designed to ensure compliance with regulatory requirements, review procedures, inventory documents, addresses all security related issues and increase security awareness at the Staff Agency/Activity level.
2. For the purposes of this security note, the enclosure and the HQMC annual assessments, the term "Commanding Officer" means "Deputy Commandant/Director"; "Command" means "Staff Agency /Activity; and "Security Manager" means "Security Coordinator".
3. Staff Agencies/Activities not meeting the requirements of the enclosure as outlined in the references will be rated Non-Mission Capable. Non-Mission Capable areas will be reevaluated in 30 days. Discrepancies not corrected after the 30 day reevaluation may affect the agencies/activities ability to continue to process, handle and/or store classified material. There are occasions where established procedures must be modified. These instances must be coordinated with HQMC (ARS) prior to implementation to ensure:
 - a. Modification will support the goals of the HQMC Information, Personnel, and Physical Security Program.
 - b. Modification does not negatively impact other agencies or organizations.
4. Staff Agency/Activity Security Coordinators will be provided with a 48 hour notification of the intended visit.

Subj: HEADQUARTERS, U.S. MARINE CORPS (HQMC) INFORMATION,
PERSONNEL, AND PHYSICAL SECURITY ASSESSMENT PROGRAM

5. HQMC Security Manager or HQMC Assistant Security Manager will conduct a Staff Agency/Activity Security Assessment out brief with the Executive Assistant.

6. Questions regarding this Security Note should be directed to ARS, at telephone (703) 614-3609.

7. This note replaces the previous version of this security note dated 14 March 2013.



R. J. GEBERTH
By direction

DETAILED INSPECTION CHECKLIST

FA	SC	STMT	TEXT
270			INFO & PERSONNEL SECURITY PROGRAM (IPSP) Functional Area Manager: PP&O Point of Contact: MR. W.T. POTTS JR. (DSN) 225-7162 (COML) (703) 695-7162 Date Last Revised: 15 October 2010
270	01		<u>ADMINISTRATION</u>
270	01	001	Does the command hold the current editions of SECNAV M-5510.36, SECNAV M-5510.30 and MCO P5510.18A? Reference SECNAV M-5510.36, EXHIBIT 2C, DOD M5200.01
270	01	002	Has the Commanding Officer issued a command security instruction? Reference SECNAV M-5510.36, PAR 2-1(5) (A); SECNAV M-5510.30, PAR 2-2(2) (F)
270	01	003	Has the Commanding Officer designated, in writing, a command security manager? Reference SECNAV M-5510.36, PAR 2-2(1); SECNAV M-5510.30 PAR 2-2(2) (A)
270	01	004	Is the Security Manager a US Citizen and been the subject of a favorably adjudicated Single Scope Background Investigation (SSBI) completed within the previous 5 years? Reference SECNAV M-5510.30, PAR 2-3(3)
270	01	005	Does the Command Security Manager have sufficient authority and staff to manage the program for the command? Reference SECNAV M-5510.30, PAR 2-3(3)
270	01	006	Is the command security manager named and identified to command personnel on command organizational charts, telephone listings, rosters, or other media? Reference SECNAV M-5510.36, PAR 2-2(3); SECNAV M-5510.30, PAR 2-3(4)
270	01	007	Does the command security manager have direct and ready access to the Commanding Officer in order to serve as the principal advisor in matters pertaining to the Command's Security Program? Reference SECNAV M-5510.36, PAR 2-2(1) (A), 2-2(3); SECNAV M-5510.30, PAR 2-3(2)
270	01	008	If applicable, has the Commanding Officer designated, in writing, additional security responsibilities as appropriate for the command? These may include: Top Secret Control Officer CNWDI Control Officer NATO Control Officer

Contracting Officer's Representative

Security Officer

Reference

SECNAV M-5510.36, PAR 2-3, 2-4 AND 2-5; SECNAV M-5510.30, PAR 2-5, 2-6 AND 2-7

- 270 01 009 Has the Commanding Officer established and maintained a self-inspection program for the command. This may include security inspections, program reviews, and assist visits to evaluate the security posture of the command?
Reference
SECNAV M-5510.36, PAR 2-1(5)(C); SECNAV M-5510.30, PAR 2-2(2)(J)
- 270 01 010 Has the Commanding Officer scheduled annual evaluations of the security posture of their subordinate commands?
Reference
SECNAV M-5510.36, PAR 2-11; SECNAV M-5510.30, PAR 2-10
- 270 01 011 Has the Commanding Officer ensured that the security manager and other security personnel receive appropriate security education and training?
Reference
SECNAV M-5510.36, PAR 2-1(5)(F); SECNAV M-5510.30, PAR 2-2(2)(H) AND PAR 2-3(5)
- 270 01 012 Has the Commanding Officer ensured that personnel are evaluated on the handling, creation or management of classified information with remarks made on performance evaluations?
Reference
SECNAV M-5510.36, PAR 2-1(5)(H); SECNAV M-5510.30, PAR 2-2(2)(K)
- 270 01 013 How are personnel in the command who perform security duties kept abreast of changes in policies and procedures?
Reference
SECNAV M-5510.36, PAR 2-2(1)(C); SECNAV M-5510.30, PAR 2-4(1)(B)
- 270 01 014 Has the command security manager formulated, coordinated, and conducted a command security education program? This includes the following briefs:
- | | |
|---------------------|--------------------------------|
| OCA Training | Derivative Classifier Training |
| Indoctrination | Annual Refresher |
| Orientation | Counterintelligence |
| On-the-Job Training | Command Debriefing |
- Reference
SECNAV M-5510.36, CHAP 3; SECNAV M-5510.30, PAR 4-4 THRU 4-11
- 270 01 015 Has the command security manager ensured threats to security, and other security violations are reported, recorded, and investigated, when necessary?
Reference
SECNAV M-5510.36, PAR 2-2, (1)(E), CHAP 12; SECNAV M-5510.30, CHAP 3
- 270 01 016 Is Security Servicing Agreements (SSA) in place for all organizations not in your command to which security services are provided?
Reference
SECNAV M-5510.36, PAR 2-10; SECNAV M-5510.30, PAR 2-11

270 02 INFORMATION SECURITY

- 270 02 001 Has the command established a Classification Management Program to ensure proper creation and handling of classified information? Specific areas of concern include original and derivative classification, declassification, and appropriate handling of various types of information, to include; Foreign Government Information, NATO, NPI, CUI, etc.
Reference
SECNAV M-5510.36, CHAP 4
- 270 02 002 Is classified information created within the command, including information residing on classified networks, appropriately marked?
Reference
SECNAV M5510.36, CHAP 6
- 270 02 003 Has the Commanding Officer approved an emergency plan for the protection and destruction of classified information?
Reference
SECNAV M-5510.36, PAR 2-1(5) (B); SECNAV M-5510.30,
PAR 2-2(2) (I) AND 2-13
- 270 02 004 If applicable, has the command security manager maintained liaison with the command Public Affairs Officer to ensure that proposed press releases and information intended for the public are subjected to a security review?
Reference
SECNAV M-5510.36, PAR 2-2(1) (H)
- 270 02 005 Has the command security manager implemented regulations concerning the disclosure of classified information to foreign nationals?
Reference
SECNAV M-5510.36, PAR 2-2(1)
- 270 02 006 Has the command security manager coordinated the preparation of command Security Classification Guides if the commander has been designated an Original Classification Authority (OCA)?
Reference
SECNAV M-5510.36, PAR 2-2(1) (G), CHAP 5
- 270 02 007 If the command is an OCA, are there established procedures to:
- Review Security Classification Guides every 5 years or as changes occur?
 - Report classification changes to cognizant holders of classified information?
- Reference
SECNAV M5510.36, PAR 4-25 AND 5-4
- 270 02 008 Has the OCA been trained, if applicable?
Reference
SECNAV M-5510.36, PAR 4-6
- 270 02 009 Has the individual specifically designated to "Act" in the OCAs absence also been trained and forwarded a letter of such training to CNO N09N2, via HQMC (PS)?
Reference
SECNAV M5510.36, PAR 4-6
- 270 02 010 Has the Commanding Officer implemented procedures for the control of Top Secret information, including working papers?
Reference

SECNAV M-5510.36, PAR 7-3 AND 7-7

- 270 02 011 Has the Commanding Officer established administrative procedures for the control of Secret and Confidential information?
Reference
SECNAV M-5510.36, PAR 7-4 AND 7-5
- 270 02 012 Has the Commanding Officer established procedures to account for, control, and mark all Secret and Confidential working papers?
Reference
SECNAV M-5510.36, PAR 7-6
- 270 02 013 Has the Commanding Officer established procedures for end of the day and after hours security checks, utilizing the SF 701, Activity Security Checklist, and the SF 702, Security Container Check Sheet, to ensure that all areas which process classified information are properly secured?
Reference
SECNAV M-5510.36, PAR 7-11
- 270 02 014 Has the command security manager ensured that all Classified information is stored in a GSA-approved security container, vault, modular vault, or secure room?
Reference
SECNAV M-5510.36, CHAP 10
- 270 02 015 Have all combinations been changed and recorded according to the provisions of the reference?
Reference
SECNAV M5510.36, PAR 10-12
- 270 02 016 Is a copy of a current SF 700, Security Container Information, affixed inside each security container, vault or secure room?
Reference
SECNAV M5510.36, PAR 10-12(4)
- 270 02 017 Have Controlled Access Areas and Restricted Areas been so Designated in writing by the Command Security Manager?
Reference
SECNAV M-5510.36, CHAP 10-3(6)
- 270 02 018 If the command has designated restricted areas, controlled access areas or open storage areas within the command, have these areas been subjected to a Physical Security Survey conducted by a school-trained, MOS 5814 Physical Security Specialist, or Civilian physical security specialist trained in accordance with the reference?
Reference
MCO 5530.14, CHAP 3, PAR 3001
- 270 02 019 Do the command's Restricted Areas meet all established requirements for the appropriate Restricted Area designation?
Reference
SECNAV M-5510.36, CH 10, EXIBIT 10A; MCO 5530.14; CNO LTR SER N09N2/10U213104, DTD 16 MAR 2010
- 270 02 020 If an IDS is utilized, was it installed by, and is it maintained and monitored as required?
Reference
SECNAV M-5510.36, EXIBIT 10D, PAR 6
- 270 02 021 If the command uses commercially provided Intrusion Detection Systems (IDS) as supplemental measures on secure spaces:

- Do they annunciate at the Provost Marshall's Office?
- Are they compatible with the Marine Corps Electronic Security Systems (MCESS) suite?

Reference

MCO 5530.14, CHAP 6

- 270 02 022 Does the command mail room have a GSA-approved security container to store USPS First Class, Certified and Registered Mail and commercial express deliveries overnight or are procedures in place to ensure these items are properly stored until a determination can be made concerning the contents?
Reference
SECNAV M-5510.36, PAR 10-3(5)
- 270 02 023 Has the Commanding Officer established procedures for the dissemination of classified and controlled unclassified information originated or received by their command?
Reference
SECNAV M-5510.36, PAR 8-1
- 270 02 024 Has the Commanding Officer ensured that only appropriately cleared personnel transmit, transport, escort, or hand carry classified information per specific requirements?
Reference
SECNAV M-5510.36, PAR 9-1 THRU 9-5
- 270 02 025 Has the Commanding Officer ensured that couriers are informed of security responsibilities when escorting or hand carrying classified information?
Reference
SECNAV M-5510.36, PAR 9-11 THRU 9-14
- 270 02 026 Has the command security manager developed security measures and procedures regarding visitors who require access to classified information? Is JPAS utilized for visit requests?
Reference
SECNAV M-5510.36, PAR 2-2(1)(J); SECNAV M-5510.30, CHAP 11; MARADMIN 077/04
- 270 02 027 Has the Commanding Officer established at least one day each year as a "clean-out" day, when specific attention and effort is focused on disposition of unneeded classified and controlled unclassified information as recommended by the reference?
Reference
SECNAV M-5510.36, PAR 10-17(2)

270 03 PERSONNEL SECURITY

- 270 03 001 Has the command security manager ensured that all personnel who have access to classified information and spaces or will be assigned to sensitive duties are appropriately cleared through coordination with DON CAF and that requests for personnel security investigations are properly prepared, submitted and monitored?
Reference
SECNAV M-5510.30, PAR 2-4(2)(F)
- 270 03 002 Has the command security manager ensured that personnel security related information and accesses are properly recorded in JPAS and local records as appropriate? Reference
SECNAV M-5510.30, PAR 2-2(L), PAR 9-1(10), APP E;
ASD (C3I) MEMO 13 JUL 00; MARADMIN 077/04

- 270 03 003 Has the command security manager ensured that all personnel who had access to classified information, who have separated or retired have completed a Security Termination Statement? Has the Security Termination Statement been forwarded to MMSB for retention?
Reference
SECNAV M-5510.30, PAR 2-4(2)(L) AND PAR 4-12
- 270 03 004 Has the command security manager ensured that all personnel execute a Classified Information Nondisclosure Agreement (SF 312) before granting initial access to classified information? Has this data been entered into JPAS and forwarded to MMSB? Is the SF 312 Pamphlet available for review if requested by the individual?
Reference
SECNAV M-5510.30, PAR 9-3
- 270 03 005 Has the command security manager ensured that all personnel granted Top Secret access have completed the Personal Attestation Statement?
Reference
SECNAV M-5510.30, PAR 4-8(5)
- 270 03 006 Has the command security manager ensured that Temporary Access (formerly Interim Clearance) authorizations are in compliance with current guidance?
Reference
SECNAV M-5510.30, CHAP 9-4
- 270 03 007 Has the Commanding officer established an administrative program for Continuous Evaluation?
Reference
SECNAV M-5510.30, CHAP 10
- 270 03 008 Are Marines who have access to classified information reported to the Naval Criminal Investigative Service (NCIS) if they are UA or in a deserter status and the command believes that their absence is contrary to national security?
Reference
SECNAV M-5510.30, PAR 3-5
- 270 03 009 Have all Commanding Officers, LtCol and above, in the unit been the subject of a favorably adjudicated Single Scope Background Investigation within the past 5 years?
Reference
SECNAV M-5510.30, PAR 7-9(1)
- 270 03 010 Have all Marines in the command been the subject of a National Agency Check with Law Agency and Credit Card Check (NACLIC) to determine enlistment or appointment suitability?
Reference
SECNAV M-5510.30, CHAP 6-5(1)
- 270 03 011 Have all government civilian employees in the command been the subject of, at a minimum, a National Agency Check with Inquiries (NACI) to determine government employment suitability?
Reference
SECNAV M-5510.30, CHAP 6-2(2)(B)
- 270 03 012 Do all instructors have a favorably adjudicated NACLIC/ ANACI, or have a waiver approved by CNO N009N2.?
Reference
SECNAV M-5510.30, CHAP 6-8(1)(D); MARADMIN 047/04

270 03 013 Have all personnel employed in or assigned to duties in IT 1, 2 or 3 positions been the subject of the appropriate background investigation?
Reference
SECNAV M-5510.30, PAR 5-3; PAR 6-8(1) (J)

270 03 014 Have all contractors working in command spaces or utilizing command IT systems been the subject of a favorably completed, command-sponsored NACI prior to issuance of a Common Access Card?
Reference
DTM 08-003, DIRECTIVE-TYPE MEMORANDUM (DTM) 08-00 "NEXT GENERATION COMMON ACCESS CARD (CAC) IMPLEMENTATION GUIDANCE"; CNO LTR SER N09N2/8U2232 DTD 29 OCT 2008; "CONTRACTOR FITNESS DETERMINATION FOR PUBLIC TRUST POSITION POLICY; "MARADMIN 098/10

270 03 015 Is the command utilizing the Joint Personnel Adjudication System (JPAS) as required, including:

- Proper establishment of the Security Management Office (SMO)?
- Proper establishment of the Personnel Security Management (PSM) Network?
- Establishment of the Parent Relationship with higher headquarters?
- Are the Security Manager and Assistant Security Manager as JPAS Account Managers?
- Are elements of the Continuous Evaluation Program reported as incidents?
- Are User IDs and Passwords being shared?

Reference
SECNAV M-5510.30, APP E; MARADMIN 077/04

270 03 016 Are appeals of DON CAF revocation/denial decisions regarding clearance eligibility being processed per the provisions of the reference?

This includes:

- Supporting the Marine as an advocate for the appeal?
- Ensuring all timelines and CAF, DOHA or PSAB requests for information are met?
- Ensuring PCS Orders are held in abeyance pending the final decision on the appeal?

Reference
SECNAV M-5510.30, CHAP 8

270 04 INDUSTRIAL SECURITY

270 04 001 Has the Commanding Officer established an industrial security program if the command engages in classified procurement or when cleared DoD contractors operate within areas under their direct control?
Reference
SECNAV M-5510.36, CHAP 11

270 04 002 Have organizational Contracting Officer Representatives (COR) been appointed in writing for the purpose of preparing and signing the "Contract Security Classification Specification" (DD Form 254) and

trained to perform their duties?

Reference

SECNAV M-5510.30, PAR 2-7; SECNAV M-5510.36, PAR 2-6

- 270 04 003 Does the COR accomplish all required responsibilities according to the reference?
Reference
SECNAV M-5510.36, PAR 11-5
- 270 04 004 Are DD254s and Visit Requests present and current to support access to classified information by contractors working within the command?
Reference
SECNAV M-5510.30, PAR 11-4(2) AND 11-4(3)
- 270 04 005 Are contractors cleared for access at levels above the Facility Clearance Level (FCL) of their employing company?
Reference
SECNAV M-5510.36, PAR 11-17
- No (Example of contractors Data Base access is not higher then JPAS access and DD 254)
- 270 05 HQMC IPSP ADDENDUM
- 270 05 001 Has the Deputy Commandant/Director ensured personnel have a critical element within their performance appraisal for evaluation of the creation, handling or management of classified information?
Reference
USD(I) Memo of 12 Jun 13 "Performance Appraisal Critical Element for the Protection of Classified Information"
- 270 05 002 Are security managers ensuring personnel who conduct derivative classifications are appropriately trained?
Reference
EO 13526 Part 2 Sec 2.1
DOD M-5200.01, VOL 3, ENCL 5 PAR 3-C & 7-C
HQMC IPSP SOP
- 270 05 003 Are security managers ensuring derivative classifications are being performed in a manner consistent with the reference.
Reference
EO 13526 Part 2 Sec 2.1
DOD M-5200.01, VOL 2
HQMC IPSP SOP
- 270 05 004 Are security managers ensuring Top Secret information and classified media created via the "write-to-media" function is entered and properly accounted for within the Classified Document Control Catalog (CDCC)?
Reference
MARADMIN 226/11
HQMC IPSP SOP
- 270 05 005 Is the reproduction of classified material (e.g. paper copies, electronic files, and other materials) only conducted as necessary to accomplish the Staff Agency/Activity mission or to comply with applicable statutes or directives?
Reference
DOD M-5200.01 VOL 3 ENCL 2 PAR 15
HQMC IPSP SOP

- 270 05 006 Are security managers ensuring personnel surrender all DoD/HQMC credentials upon check out? Are security coordinators turning these items into the Security Office once collected?
Reference
HQMC IPSP SOP
- 270 05 007 Has the Deputy Commandant/Director ensured submissions of a Single Scope Background Investigation (SSBI), Single Scope Background Investigation Periodic Reinvestigation (SBPR) and Phased Periodic Reinvestigation (PPR) are submitted for billets coded appropriately in the Total Force Structure System (TFSMS), MOS designated or cases approved via the waiver process?
Reference
SECNAV M-5510.30 PAR 6-1, 6-4, 6-6
GENADMIN MSG 101326Z JUN 11
HQMC IPSP SOP
- 270 05 008 Has the Deputy Commandant/Director provided combinations for secure office space exterior doors via SIRPNET to ARS?
Reference
SECURITY NOTE 03-13
- 270 05 009 Has the Deputy Commandant/Director submitted all requests for the installation or repair of all locking devices (i.e. X09 Container Locks, CD X09 door combination locks, Simplex mechanical locks, Unican E-Plex 2000 mechanical push button Locks and AMAG) to ARS?
Reference
SECURITY NOTE 07-10
- 270 05 010 Is the Staff Agency/Activity access roster posted on the interior wall of a designated space adjacent to the main entry point and is not be visible from the exterior?
Reference
MCO 5530.14A
HQMC IPSP SOP
- 270 05 011 Does the staff agency/activity have a valid Accreditation Letter (AL) on file? If not, has the security manager routed a request for the AL through the Physical Security Specialist?
Reference
DOD M-5200.01, VOL 3 ENCL 3 PAR 3
MCO 5530.14A